DEPARTMENT OF TECHNOLOGY & INFORMATION

DELIVERING TECHNOLOGY THAT INNOVATES

eSecurity News—Pharming and SMiShing and Vishing, Oh My!

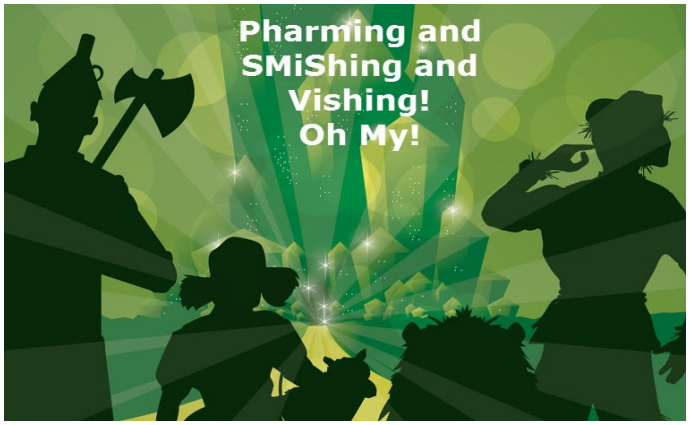
Technology is often used by criminals to attempt to fool people into parting with their **Personally Identifiable Information** (**PII**). PII consists of passwords, bank account and routing numbers, credit card numbers, birth dates, social security numbers, medical information or other highly-personal identification data. Criminals want PII to commit Identity Theft, raid bank accounts, obtain fake identification documents, insurance, credit, loans and other goods or services.

Phishing is using a false identity, often posing as a bank, legal entity or legitimate organization to coax people into opening an email. The fraudster tries to trick the recipient into providing PII, account access information or to deliver malware packages. These attacks use realistic-looking services such as websites, email, text messaging, social media and phone calls to conduct malicious activities.

DigiKnow that one way we reduce the risk of Phishing attacks is to conduct Phishing exercises designed to educate and increase awareness? Based on the reduced numbers of people clicking on Phishing emails—it's working!

Pharming directs an Internet user to a bogus website mimicking the appearance of a legitimate one. It is set up to obtain PII. Be especially careful when entering financial information on a website. Be suspicious if the website looks different than when you last visited and don't click unless you are certain the site is secure. To avoid becoming a victim of Pharming, follow the basic computer safety guidelines in Protect Your Computer.

SMiShing is a close cousin of Phishing that uses SMS text messages on cellphones and smartphones instead of emails. For tips to protect yourself from SMiShing attacks visit Lifewire.com.



Vishing is the practice of making fraudulent calls or leaving voice messages purporting to be from reputable companies in order to coax individuals to provide personal information.

Some of these attempt to get you to verbalize "Yes" by asking, "Can you hear me?" or some similar yes-or-no question. The voice recording of "Yes" can be used as "proof" that you agreed to a purchase or service.

These criminals use caller ID spoofing (using computers to fake the number the call is from) to imitate trusted area codes. Scammers can collect long distance charges from you if you return calls to numbers you don't recognize. Seniors are often targeted for Vishing.

Regardless of what it's called or the attack method used, these fraudulent Phishing activities are crimes. At work know and abide by your organization's security practices and at home take steps to protect your family. Visit Cyber Security in Delaware, the Federal Trade Commission (FTC), security sites for your particular computer or mobile device and other reputable sites to become an educated technology consumer.

Visit scam-detector.com to read more information on avoiding these and other common scams.

Questions, comments or topic suggestions? Email us at eSecurity@state.de.us

Visit the DTI eSecurity website for previous issues of eSecurity Newsletters

DigiKnow
CYBER SECURITY DEPENDS ON YOU

This newsletter is published by the Delaware Department of Technology and Information and sent to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or would like a printable copy (PDF), go to http://extranet.dti.state.de.us/information/